REMARKS

Claims 24, 28, 30, 33-35, 37, 40-43, and 45-51 are pending. Note that claim 44 was previously canceled. Claims 24, 28, 30, 33-35, 37, 40, 42, 43, 45, 50, and 51 are rejected under 35 USC 103(a) as being unpatentable over U.S. patent 7,215,775 (Noguchi et al.) in view of U.S. patent 6,947,559 (Gleeson). Claim 41 is rejected under 35 USC 103(a) as being unpatentable over Noguchi in view of Gleeson and U.S. patent application publication 2002/0154769 (Petersen et al). Claim 46 is rejected under 35 USC 103(a) as being unpatentable over Noguchi in view of Gleeson, and in view of Petersen, and in view of U.S. patent 6,973,499 (Peden).

Claims 52 and 53 are new. Claims 24, 33, 35, 40, 42, 43, and 47 are amended. No new matter is added. Claims 24, 28, 30, 33-35, 37, 40-43, and 45-53 are presented for examination. Claims 24, 40, and 47 are independent.

Description of claim amendments

The term "the Internet" is replaced with "a public communication network", as supported below. This terminology was previously recited in claim 41.

Applicants' [0009] lines 1-2: "*According to the invention, a symmetrical encryption method is used for the protected data transmission, for example over a public communication network such as the internet.*"

The independent claims now recite remote users, as supported in par. [0024]. "Remote" is known in the field of data communications to mean "at different locations" -- certainly not in the same room, as is required for the principle of operation of Noguchi.

New claim 52 is supported by paragraph [0022].

New claim 53 is supported by paragraphs 61 - 67 and FIG 5.

No new matter is added to the disclosure by these amendments.

Response to rejections under 35 USC 103(a)

The term "useful data" is well known in the field of data communications to mean the net payload of data communicated to a receiver, exclusive of any protocol overhead. This is how the term is defined and used in the present specification.

> Applicants' par [0016] lines 3-7: "*For example, a corresponding request is made when the utilization of the capacity of the communication network for useful data (payload) transmission is relatively low, in order then to use the unused bandwidth for transmitting data as a basis for the key generation in the users.*"

Common usage of this term is exemplified in Wikipedia in the "Bit Rate" topic: "*In digital communication systems, the gross bitrate, raw bitrate, line rate or data signaling rate is the total number of physically transferred bits per second over a communication link, including useful data as well as protocol overhead* ". Protocol overhead is known to include such items as encryption keys, CRC check bytes, transmission packet address bits, control frames, etc. -- in other words, any overhead bits used for transmitting the payload.

In par. 11 of the office action of 05/27/2009, Examiner ignores the first three steps (a, b, c) of Noguchi, and starts at step (d) for comparison with Applicants' claimed invention. However, this modification changes the principle of operation of Noguchi, the purpose of which is visual verification of transmission integrity of a public key. This is the whole point of Noguchi, as recited in the abstract.

> *MPEP 2143.01 VI. THE PROPOSED MODIFICATION CANNOT CHANGE THE PRINCIPLE OF OPERATION OF A REFERENCE*
> *If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims prima facie obvious. In re Ratti, 270 F.2d 810, 123 USPQ 349 (CCPA 1959)*

Noguchi requires the sending and receiving terminals to be in the same room for direct visual comparison of verification displays on both terminals by a user. This makes Noguchi

inoperable for users remote from each other. All of the independent claims are amended herein to recite remote users.

> Noguchi col. 4, lines 48-52: "*The distance between both the data send/receive devices is typically less than 10 m, preferably several meters, such that a user can come and go, since the verification data needs to be compared mutually at the verification data output sections of both the data send/receive devices.*"

> Noguchi col. 9, lines 33-40: "*(c) Users of source A and destination B verify whether verification data Xp and Xx that are displayed in the respective displays are the same. If Xp equals Xx, this means Kx equals Kp, hence it is determined that data integrity is assured for the communication path between source A and destination B.*"

All of the independent claims herein recite "useful data" as the source of stochastic data. This omits the need for a specialized stochastic random number generator such as that of Gleeson in the proposed combination, while retaining the function thereof.

> Applicants' par. [0043]: "*Alternatively, the data supplied by the data source 116 can also be used as stochastic data as a basis for generating the symmetrical key. This is advantageous in particular when the data source 116 supplies measured values of quantities or parameters that vary over time, of an automation system for example. For example, certain process parameters in an automation system of said kind, such as the temperature, pressure, speed of rotation, etc., are not deterministic, but more or less random with more or less periodic components. A corresponding measured value supplied by the data source 116 can therefore be used as a stochastic datum for symmetrical key generation, a separate acquisition module 112 or, as the case may be, an additional stochastic process 114 being superfluous in this case.*"

> MPEP 2144.04 II B.: "*Omission of an Element with Retention of the Element's Function Is an Indicia of Unobviousness. In reEdge, 359 F.2d 896, 149 USPQ 556 (CCPA 1966)*"

On top of page 5 of the Office Action, Examiner cites Noguchi col. 13, line 65 to col. 14, line 2 as teaching use of the Internet or other large networks. This is not found. These lines simply teach that the method can be implemented on one computer system, or on several interconnected computer systems. He does not teach that any of the interconnected computer

systems are remote. It is common for computer systems in the same room to be interconnected by an Ethernet LAN. Noguchi is clearly inoperable for remote users as argued above.

In par. 24 of the Office Action, Examiner holds it obvious to transmit data over the Internet at times of low utilization. However, claim 35 does not recite transmitting useful data during low network utilization. It recites transmitting a random value for use as an encryption key. This can be done any time. In Noguchi, transmitting the random value can only be done when a person is physically available for visual verification. It is impractical for a person to wait for low network utilization to do this. Furthermore, Noguchi does not teach how to provide such an interruption to a user.

In par. 35 of the Office Action, Examiner cites Noguchi Fig 13, col. 13, lines 48-63 as teaching use of a public network. His embodiment of Fig 13 does not make his method operable by users remote from each other. The two PDA users still must visually verify the verification display by looking at both PDAs, which means they must be at the same location.

In paragraphs 32 and 33 of the Office Action, Examiner cites Gleeson col. 3, lines 47-62 as teaching combining at least two digital values from different operational measurements to create a random number. This is not found. Gleeson states "*The present invention is directed to a method and apparatus for the generation of random numbers based on chaotic, turbulent flow, which is well known for its random behavior. Such flows ate highly nonlinear, in that very many spatial and temporal Fourier modes are strongly coupled and so are continually mixing.*" This is merely a description in mathematical terms of the randomness of a turbulent flow, and does not teach combining or concatenating digital values from two or more operational measurements to obtain a random number.

In par. 22 of the office action, Examiner cites Gleeson col. 3, lines 44-62 as teaching that first and second symmetrical encryption keys are generated at predetermined times or after a lapse of a predetermined time interval. However, this is not found in the cited lines. They describe chaotic and unpredictable processes that can form the basis for random numbers, but not generating encryption keys a predetermined times or predetermined intervals.

Regarding claim 41: Examiner asserts that it would be an obvious design choice to use the least significant bits of measured data to generate an encryption key. In par. 37 of the Office Action, he refers to Petersen par. 39. However par. 39 of Petersen teaches <u>avoiding</u> deletion of high order bits of data, explicitly teaching away from Applicants' method of claim 41. Loss of high order bits is an overflow condition, which is a "fatal" or terminal error, and is displayed as such on all calculators.

> Petersen par. 39, lines 6-12 : *"The position of the decimal separator in a fixed-point number is a weighting between digits in the integer part and digits in the fraction part of the number. To achieve the best result of a calculation, it is usually desired to include as many digits after the decimal separator as possible, to obtain the highest resolution. <u>However, it may also be important to assign enough bits to the integer part to ensure that no overflow will occur. Overflow is loading or calculating a value into a register that is unable to hold a number as big as the value loaded or calculated. Overflow results in deletion of the most significant bits (digits) and possible sign change.</u>"*

A design choice is one of several known options that are similarly good choices. However, removing high-order bits from useful measurement data destroys the data. For example, assume a time series of 8-bit measurement data has a range from binary 00100101 to 01110011 (decimal 37 to 115). If you remove the top 2 bits, the data is limited to a maximum value of 111111, or decimal 63. This causes an overflow for any values greater than 63, which destroys the data, and thus would certainly not be done without some non-obvious reason. Furthermore, the goal of a random number is unpredictability. The more significant bits there are in a random number, the less predictable and more secure it is as a seed value for an encryption key. This teaches away from using only the least significant bits, either for data or for security key generation. For these reasons, the method of claim 41 is not supported by general knowledge, and is not an obvious design choice.
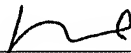
Conclusion

M.P.E.P. 2143.03 provides that to establish prima facie obviousness of a claimed invention, all words in a claim must be considered in judging the patentability of that claim against the prior art. If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious.

As argued above, the proposed combinations lack features claimed in the independent claims and others herein. Furthermore, the proposed combinations must change the principle of operation of the main reference. Furthermore, the proposed combinations must add an element that is omitted in the present invention without loss of function. Thus the proposed combinations do not support the obviousness rejections of the claimed invention. Applicants feel this application is in condition for allowance, which is respectfully requested.

The commissioner is hereby authorized to charge any appropriate fees due in connection with this paper, including fees for additional claims and terminal disclaimer fee, or credit any overpayments to Deposit Account No. 19-2179.

Respectfully submitted,

Dated: 08/19/09   By: _____

                                   Ye Ren
                                   Registration No. 62,344
                                   (407) 736-6844

Siemens Corporation
Intellectual Property Department
170 Wood Avenue South
Iselin, New Jersey 08830